UNITED STATES OF AMERICA

CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

MARCH 2020

CSC FINAL REPORT

IMPACT ON MEDICAL DEVICE MANUFACTURERS

SPONSORED BY

VIGILANT OPS, INC.

PRESENTED BY

KEN ZALEVSKY

ABOUT THE SPEAKER – KEN ZALEVSKY

- Chief Executive Officer, Vigilant Ops, Inc.
- Vigilant Ops is a medtech company specializing in medical device security and the developer of the InSight Platform
- The InSight Platform is used by Medical Device Manufacturers to automatically generate, maintain and share Software Bill of Materials (SBOM)
- The InSight Platform is used by Healthcare Delivery Organizations to consume SBOMs and monitor deployed device vulnerabilities

THE CYBERSECURITY THREAT

- NotPetya cyber attack originated in Ukraine in June 2017
- Destructive malware exploiting vulnerabilities in Microsoft Windows OS
- Quickly spread across industries and businesses including hospitals and medical device manufacturers
- Losses estimated to be $10 Billion
- ***A more connected world is also a more vulnerable world***

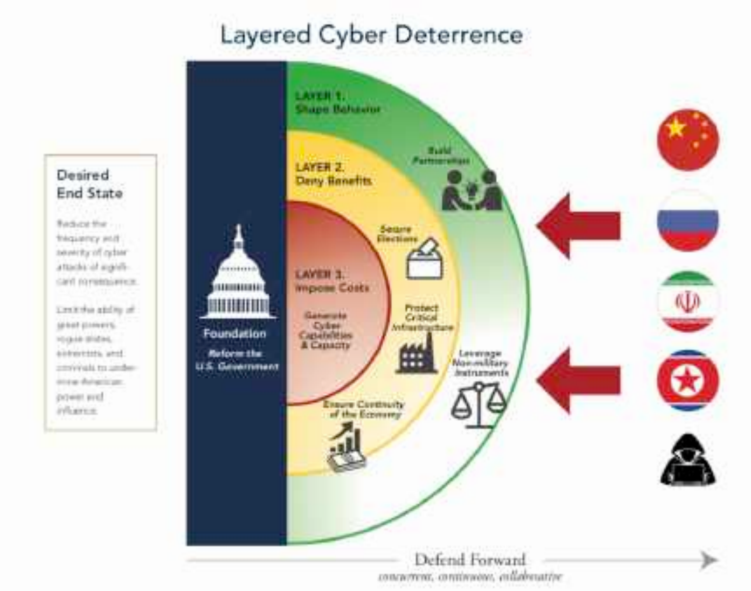
CYBERSPACE SOLARIUM COMMISSION

UNITED STATES OF AMERICA
CYBERSPACE
SOLARIUM
COMMISSION

- 2019 National Defense Authorization Act chartered CSC in 2019
- US President and Congress tasked CSC with two questions
    - What strategic approach will defend the United States against cyberattacks of significant consequence?
    - What policies and legislation are required to implement that strategy?
- Published Final Report on March 11, 2020 – 80+ recommendations
- 2021 Fiscal Year Legislative Proposals on July 14, 2020 – 54 legislative proposals
- ***"The status quo in cyberspace is unacceptable."***
- ***"Adversaries are increasing their cyber capabilities while US vulnerabilities continue to grow."***
- ***"If the US government cannot find a way to seamlessly collaborate with the private sector to build a resilient cyber ecosystem, the nation will never be secure."***

CSC PROPOSES LAYERED CYBER DETERRENCE

- Shape Behavior
  - Working with allies and partners to promote responsible cyber behavior
- Deny Benefits to Adversaries
  - Secure critical networks in collaboration with the private sector to increase ecosystem security
- Impose Costs
  - As a deterrent and motivator



Layered Cyber Deterrence

Desired End State

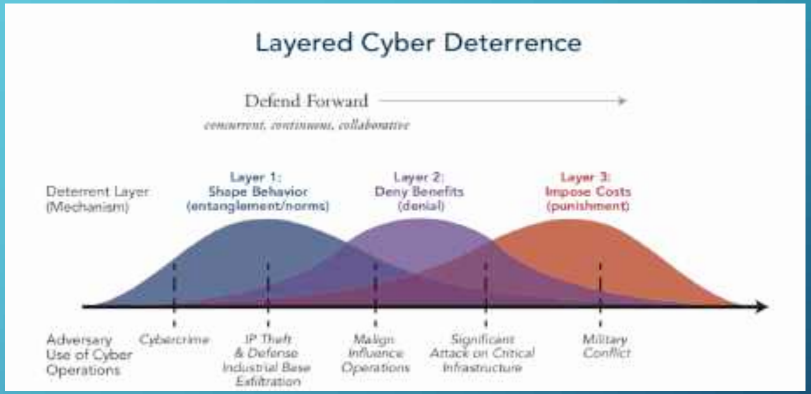
Reduce the frequency and severity of cyber attacks of significant consequence.

Limit the ability of great powers, rogue states, extremists, and criminals to undermine American power and influence.

Foundation
Reform the U.S. Government
LAYER 1. Shape Behavior
LAYER 2. Deny Benefits
LAYER 3. Impose Costs
Build Partnerships
Secure Elections
Generate Cyber Capabilities & Capacity
Protect Critical Infrastructure
Leverage Non-military Instruments
Ensure Continuity of the Economy
Defend Forward
concurrent, continuous, collaborative

CYBER DETERRENCE CONCEPT DETAILS

- Deterrence by Denial
  - By increasing defense and security of cyberspace
  - ***Through public and private sector collaboration***
  - Reducing vulnerabilities reduces targets for adversaries


Layered Cyber Deterrence
Defend Forward
concurrent, continuous, collaborative
Deterrent Layer (Mechanism)
Layer 1: Shape Behavior (entanglement/norms)
Layer 2: Deny Benefits (denial)
Layer 3: Impose Costs (punishment)
Adversary Use of Cyber Operations
Cybercrime
IP Theft & Defense Industrial Base Exfiltration
Malign Influence Operations
Significant Attack on Critical Infrastructure
Military Conflict

- Defend Forward
  - Reducing frequency and severity of attacks
  - Proactively pursuing and countering all levels of attacks

STRATEGY BUILT ON SIX (6) PILLARS

- Reform the US government’s structure and organization for cyberspace
- Strengthen norms and non-military tools
- Promote national resilience
- Reshape the cyber ecosystem
- Operationalize cybersecurity collaboration with the private sector
- Preserve and employ the military instrument of power

REFORM THE US GOVERNMENT'S STRUCTURE AND ORGANIZATION FOR CYBERSPACE

- *"The recommendations in this pillar are intended to provide the US government with the strategic continuity and unity of effort necessary to support the other pillars and recommendations of this report in achieving layered cyber deterrence and defending US critical infrastructure against cyberattacks of significant consequence."*

REFORM THE US GOVERNMENT – STRATEGIC OBJECTIVES

1. Align US government strategy with layered cyber deterrence
    a. Update the National Cyber Strategy
2. Streamline congressional oversight and authority over cybersecurity issues
    a. Consolidate cybersecurity budget and legislative jurisdiction
3. Reform the Executive branch to be more agile and effective in cyberspace
    a. Establish the position of National Cyber Director as principal advisor to the President
4. Recruit, develop, and retain a stronger federal cyber workforce
    a. Deepen and diversify the pool of candidates for cyber work in the federal government

STRENGTHEN NORMS AND NON-MILITARY TOOLS

- *"Norms, which are collective expectations for the proper behavior of actors with a given identity, already exist in cyberspace but can be bolstered by building on the United States' network of international allies and partners and their shared commitment to enforcing those expectations."*

STRENGTHEN NORMS – STRATEGIC OBJECTIVE

1. Expand efforts through international engagement to strengthen and reinforce norms in cyberspace
   a. Create a broad, like-minded community of allies and partners
   b. Maintain and reinforce norms that underpin a favorable cyber landscape
   c. Create and resource the Bureau of Cyberspace Security and Emerging Technologies (CSET)
   d. Improve international tools for law enforcement activities in cyberspace

PROMOTE NATIONAL RESILIENCE

- *“Resilience – the capacity to withstand and quickly recover from attacks that could compel, deter, or otherwise shape US behavior – is a foundational element of layered cyber deterrence, ensuring that critical functions and the full extent of US power remain available in peacetime and are preserved in crisis.”*

PROMOTE NATIONAL RESILIENCE – STRATEGIC OBJECTIVES

1. Understand, assess, and manage national risk
   a. Ensure sufficient resources for Cybersecurity and Infrastructure Security Agency (CISA)
   b. Establish a five-year national risk management cycle
   c. Establish a National Cybersecurity Assistance Fund, directed by CISA
2. Ensure national capacity to respond and recover from a significant cyber incident
   a. Improve cyber incident response, establish a biennial national tabletop exercise (e.g. Cyber Storm)
3. Ensure the security of our elections and resilience of our democracy
   a. Improve structure and modernize campaign regulations to promote cybersecurity

RESHAPE THE CYBER ECOSYSTEM

Drive down vulnerability by shifting the burden of security to manufacturers

- *"This pillar attempts to **drive down vulnerability** across the ecosystem **by shifting the burden of security** away from end users **to** owners, developers, and **manufacturers** who can more efficiently implement security solutions at the appropriate scale."*

RESHAPE CYBER ECOSYSTEM – STRATEGIC OBJECTIVES

1. Incentivize greater security in the markets for technology
   a. Incentivizing product manufacturers to adopt a “secure to market” strategy
2. Incentivize better organizational cybersecurity
   a. Update cybersecurity regulations in the Federal Acquisition Regulations to help develop and generate cybersecurity industry best practices and standards
   b. Amend Sarbanes-Oxley Act to include cyber reporting requirements
3. Empower information and communications technology enablers to deploy security across the ecosystem
   a. Incentivize (tax breaks) the uptake of secure cloud services for small and medium-sized businesses
4. Reduce critical dependencies on untrusted information and communications technology
   a. Commit significant funding toward R&D in emerging technologies (National Cyber Moonshot Initiative)
5. Strengthen national systemic data security
   a. National law to establish requirements for collection, retention and sharing of user data

INCENTIVIZING A “SECURE TO MARKET” STRATEGY

Key Recommendation 4.1

Congress should establish and fund a National Cybersecurity Certification and Labeling Authority empowered to establish and manage a program for voluntary security certifications and *labeling of information and communications technology products*

”Without accessible and transparent mechanisms, such as certifications (e.g. Energy Star, Underwriters Laboratory, or Certified Organic products) and labels (e.g. nutrition labels), to compare security between products, critical infrastructure owners and operators cannot easily price security into their purchasing decisions.”

NATIONAL CYBERSECURITY CERTIFICATION AND LABELING AUTHORITY

1. Product certification and attestation
   a. Publicly certify products that vendors have attested meet and comply with cybersecurity standards
2. Accredited certifying agents
   a. Define criteria and process for accrediting non-governmental organizations as certifying agents
   b. Medical device certifying agent?
3. Comparative security scoring
   a. Coordinate with NIST to refine security scoring metrics
4. Partnership on product labeling
   a. Develop a labeling regime to provide transparent information on the characteristics and constituent components of a software or hardware product
   b. Specifically include those components that contribute to the security of a product
   c. Establish a mechanism to educate end users about the component characteristics
   d. Provide component security information as product labeling and public posting

PROVIDING TRANSPARENT COMPONENT SECURITY INFORMATION

Ingredients: Aqua, Ammonium Lauryl Sulfate, Decyl Glucoside, Lauryl Glucoside, Cocamidopropyl Betaine, Dimethicone (and) Amodimethicone (and) Laureth-23 (and) Polyquaternium-10 (and) Laureth-4, Glycol Distearate, Acrylates Copolymer, Polyquaternium-7, Fragrance, PEG 150 Distearate, Citric Acid, Polyquaternium-10, Potassium Sorbate, Sodium Benzoate, Glycerin, Disodium EDTA, Maltooligosyl Glucoside & Hydrogenated Starch Hydrolysate, PEG-45M, Methylchloroisothiazolinone & Methylisothiazolinone, Sodium Hydroxide, BHT, Cicer Arietinum Seed Extract, Terminalia Bellerica Fruit Extract.

FOR EXTERNAL USE ONLY. Store in a cool and dry place. Clinically proven for effectiveness.

For Mfg. Lic. No., M.R.P.Rs. Incl. of all taxes, Batch No. &

- Software Bill of Materials (SBOM)
  - Inventory of all software components running in a product
  - Generated and maintained by the final goods assembler (product manufacturer)
  - Gaining traction and attention as a product security best practice
    - ***FDA* –** medical device SBOM
    - **ANSI/NEMA -** MDS^2 (Manufacturer Disclosure Statement for Medical Device Security)
    - **NTIA –** standardization of the SBOM format across multiple industries

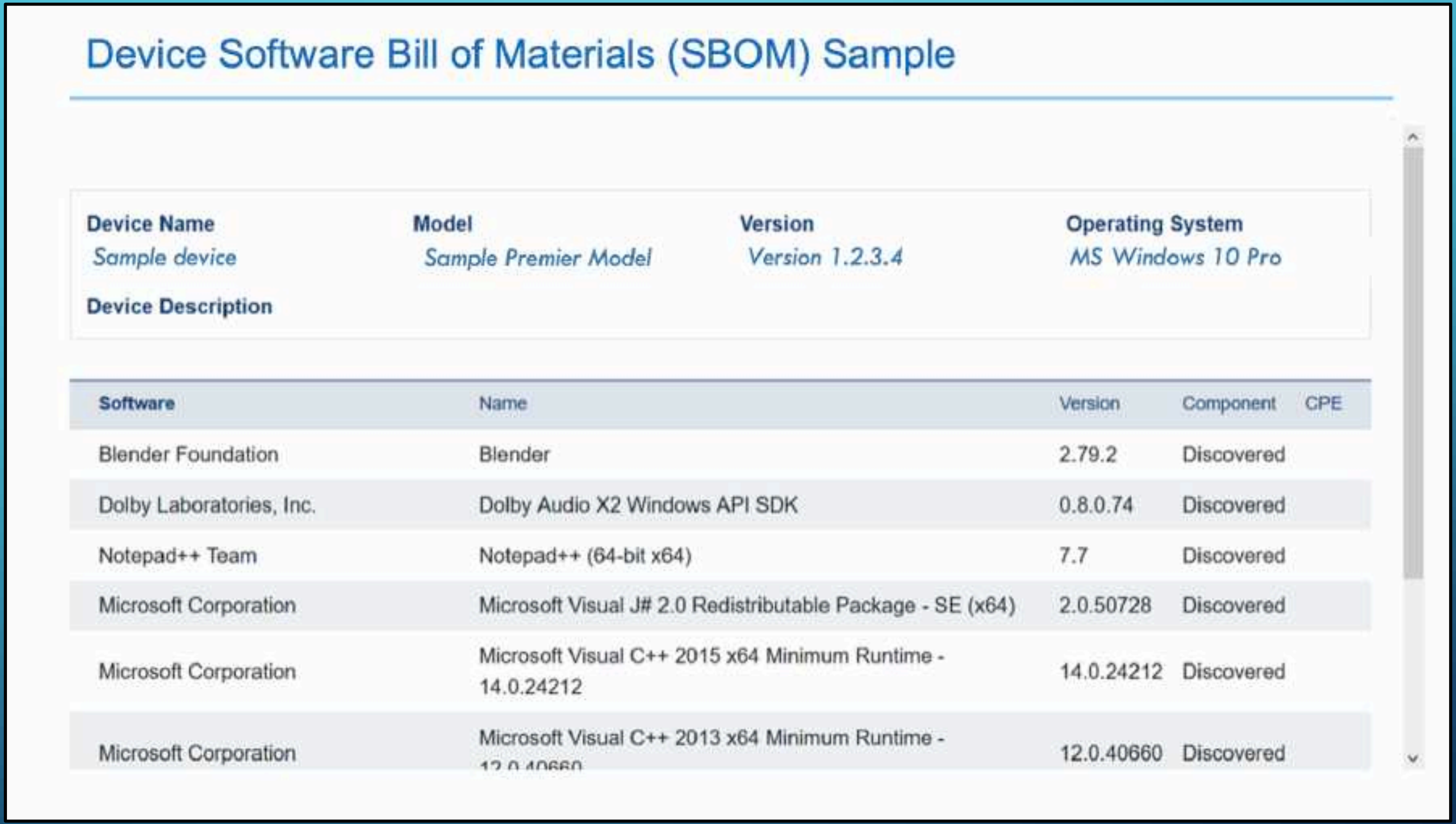
INCENTIVIZING A “SECURE TO MARKET” STRATEGY

Key Recommendation 4.2

Congress should pass a law establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities.

”Congress should direct the Federal Trade Commission to establish a regulation mandating transparency from final goods assemblers.”

TRANSPARENCY OF MEDICAL DEVICES



Device Software Bill of Materials (SBOM) Sample

Device Name	Model	Version	Operating System
Sample device	*Sample Premier Model*	*Version 1.2.3.4*	*MS Windows 10 Pro*

Device Description

Software	Name	Version	Component	CPE
Blender Foundation	Blender	2.79.2	Discovered	
Dolby Laboratories, Inc.	Dolby Audio X2 Windows API SDK	0.8.0.74	Discovered	
Notepad++ Team	Notepad++ (64-bit x64)	7.7	Discovered	
Microsoft Corporation	Microsoft Visual J# 2.0 Redistributable Package - SE (x64)	2.0.50728	Discovered	
Microsoft Corporation	Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24212	14.0.24212	Discovered	
Microsoft Corporation	Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660	12.0.40660	Discovered	

ENABLING RECOMMENDATIONS

1. Create or designate (up to 3) critical technology security centers
   a. Evaluating and testing security of devices and technology critical to national infrastructure
2. Expand and support National Institute of Standards and Technology (NIST) security work
   a. Routinely update cybersecurity frameworks, including the NIST Cybersecurity Framework
   b. Develop and harmonize standards for secure technology development
   c. Develop and harmonize standards for vulnerability and patch management
   d. Provide lasting support for the National Vulnerability Database (NVD), Common Vulnerability Exposures (CVE) program, and the Cybersecurity and Infrastructure Security Agency's (CISA) vulnerability disclosure work

ENABLING RECOMMENDATIONS

1. Incentivize timely patch implementation
   a. Vulnerability discovery, disclosure, and patch development do little when patches go unimplemented
   b. Usually due to challenge of implementing patch within the user’s environment
   c. Scheduling downtime causes issues and loss of productivity

LEGISLATIVE PROPOSAL 4.2
ESTABLISH LIABILITY FOR FINAL GOODS ASSEMBLERS

- **Final Goods Assembler**
  - Entity most responsible for placement of product into stream of commerce
- **Private Right of Action – Damages Up to 15% of Annual Revenue**
  - End users may bring action against final goods assemblers not meeting ***standard of care***
- **Standard of Care**
  - Makes security patches available within *90 days of a vulnerability*[2]
    - ***Being disclosed through the National Vulnerability Databased (NVD) and including, but not being limited to, being assigned a Common Vulnerabilities and Exposures number***

[2] No distinction of criticality or risk of vulnerability, whereas FDA categorizes Controlled and Uncontrolled Risk in their Postmarket Guidance

OPERATIONALIZE CYBERSECURITY COLLABORATION WITH THE PRIVATE SECTOR

- *“This pillar attempts to operationalize cybersecurity collaboration with the private sector by organizing and focusing US government efforts on areas where they can have an outsized impact.”*

OPERATIONALIZE – STRATEGIC OBJECTIVES

1. Improve government support to private sector operations
   1. US government and private sector have incentive to protect critical systems and assets
   2. Congress should codify into law the concept of “systemically important critical infrastructure”
   3. Entities responsible for systemically critical systems and assets are granted special assistance from the U.S. government
   4. Entities shoulder additional security and information sharing requirements befitting their unique status (Healthcare)
2. Improve combined situational awareness of cyber threats
   1. Pass a national cyber incident reporting law
3. Integrate public and private sector defense efforts for better coordinated incident response

PRESERVE AND EMPLOY THE MILITARY INSTRUMENT OF POWER

- *"This pillar comprises implementing defend forward in day-to-day competition to counter adversary cyber campaigns and impose costs, as well as being prepared to prevail in crisis and conflict."*

PRESERVE MILITARY POWER – STRATEGIC OBJECTIVES

1. Grow the capacity of the Cyber Mission Force (CMF) to meet the scope of the threat and growing mission requirements
   a. Congress should direct the Department of Defense to conduct a force structure assessment of the Cyber Mission Force (CMF)

2. Ensure the security and resilience of critical conventional and nuclear weapons systems and functions

SUMMARY OF REPORT KEY POINTS

- Cybersecurity posture across US industries is weak and not sustainable
- US government currently not structured to handle cybersecurity – recommend new/revised roles and responsibilities
- Recommend several public-private joint initiatives
- Some current initiatives are working, just need to provide additional funding and continued support
- Propose shifting the burden of security away from end users to manufacturers
- Incentivizing (punishing) manufacturers for compliance (non-compliance)
- Information technology products should include component security information (transparency)

TAKEAWAYS FOR MEDICAL DEVICE MANUFACTURERS

Drive down vulnerability by shifting the burden of security to manufacturers

- Be Responsive
  - Adhere to communication and patch mandates
  - 15% of annual revenue could be substantial

- Be flexible with security vulnerability scoring system
  - Common Vulnerability Scoring System (CVSS) updates?
  - Clearly identify scoring impact in policies/procedures and be prepared to modify

- Be ready to provide SBOM (Software Bill of Materials) with products
  - Develop and implement SBOM processes
    - Generate and maintain SBOMs for each unique product version
    - Monitor SBOM component vulnerabilities
    - Share SBOMs with authorized end users

RESOURCES

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA, October 2018 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices

- Postmarket Management of Cybersecurity in Medical Devices, FDA, December 2016 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

- NTIA SBOM - https://www.ntia.doc.gov/SoftwareTransparency

- NEMA MDS^2 - https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security

- Cyberspace Solarium Commission - https://www.solarium.gov

- Vigilant Ops – www.vigilant-ops.com

INSIGHT PLATFORM DEMONSTRATION